UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/652,415	08/31/2000	Osamu Kobayashi	GNSS-0019	4253

22434 7590 03/15/2004

BEYER WEAVER & THOMAS LLP
P.O. BOX 778
BERKELEY, CA 94704-0778

EXAMINER	
SHERKAT, AREZOO	

ART UNIT	PAPER NUMBER
2131	8

DATE MAILED: 03/15/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/652,415	KOBAYASHI ET AL.	
	Examiner	Art Unit	
	Arezoo Sherkat	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 August 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☒ Claim(s) *17* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 August 2000* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *5*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-17 have been presented for examination.

Drawings

New corrected drawings are required in this application because Figure 2 and Figure 3 are not formal. Applicant is advised to employ the services of a competent patent draftsperson outside the Office, as the U.S. Patent and Trademark Office no longer prepares new drawings. The corrected drawings are required in reply to the Office action to avoid abandonment of the application. The requirement for corrected drawings will not be held in abeyance.

Allowable Subject Matter

Claim 17 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-4, and 12-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shimizu et al., (U.S. Patent No. 6,085,323 and Shimizu hereinafter), in view of Ashe, (U.S. Patent No. 6,014,745 and Ashe hereinafter).

Regarding claim 1, Shimizu discloses a method of using an unencrypted key, said method comprising:

encrypting said unencrypted key (i.e., temporary key generated by the random number generator 3) according to an encryption protocol to generate an encrypted key (i.e., the encrypting device 10 encrypts the transferred temporary key using a master key stored in a master key memory 9)(Col. 7, lines 13-22);

storing said encrypted key in a non-volatile memory (i.e., the header portion 11 and the body portion 8 is stored in the storage device 12)(Col. 7, lines 26-30);

Shimizu does not expressly disclose decrypting and using the unencrypted key in the same integrated circuit.

However, Ashe discloses:

retrieving said encrypted key (i.e., Zi, the encrypted Kc) into an integrated circuit (i.e., DSP, Digital Signal Processor) when said unencrypted key is required for use, decrypting said encrypted key in said integrated circuit to generate said unencrypted key (i.e., deciphering Zi with the master decryption algorithm module21), and using said unencrypted key (i.e., after the key Kc is deciphered, the DSP reads the encrypted

program y with the customer decryption algorithm module 23)(Col. 2, lines 65-67 and Col. 3, lines 1-10).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Shimizu with the teachings of Ashe to include an integrated processing unit such as a Digital Signal Processor (DSP), that has both the proprietor's unique algorithm (i.e., unencrypted key), master algorithm (i.e., encryption protocol), and master key (i.e., the key to encrypt the unencrypted key) with the motivation to protect information stored in a memory device (Ashe, Col. 1, lines 1-10).

Regarding claim 2, Shimizu discloses random number generator 3 may be in IC card 5 instead of portable PC 6, then the extracted temporary key can be used in decrypting device 20 to decrypt the body portion 8 in the IC card itself instead of it being transferred to decrypting device 14 in portable PC 6)(Col. 7, lines 23-30 and Col. 8, lines 8-25).

Shimizu does not expressly disclose wherein said unencrypted key is used within said integrated circuit.

However, Ashe discloses wherein said unencrypted key (i.e., deciphered Zi, Kc) is used (i.e., reading the encrypted program Y with the customer decryption algorithm module 23) within said integrated circuit (i.e., DSP)(Col. 2, lines 65-67 and Col. 3, lines 1-10).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Shimizu with the teachings of Ashe to include an integrated processing unit such as a Digital Signal Processor (DSP), that has both the proprietor's unique algorithm (i.e., unencrypted key), master algorithm (i.e., encryption protocol), and master key (i.e., the key to encrypt the unencrypted key) with the motivation to protect information stored in a memory device (Ashe, Col. 1, lines 1-10).

Regarding claim 3, Shimizu does not expressly disclose wherein said unencrypted key comprises an authentication key and said using comprises authenticating a source of data.

However, Ashe discloses wherein said unencrypted key comprises an authentication key (i.e., Kc, decrypted Zi) and said using comprises authenticating a source of data (i.e., verification that the entered key is the same as the encrypted key and allowing card holder to conduct transaction and obtaining cash via dispenser 26)(Col. 3, lines 15-38 and Col. 4, lines 1-15).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Shimizu with the teachings of Ashe to include a microprocessor similar to DSP as part of a smart card system, the memory, equipped with conductors, mounted on a card to be inserted in a slot with the motivation to allow a machine such as a cash machine having a microprocessor mounted within it to read the memory and verify that the key card holder enters is the

same as the encrypted key and allow the card holder to conduct transaction (Ashe, Col. 3, lines 15-36).

Regarding claim 4, Shimizu discloses wherein said unencrypted key (i.e., temporary key generated by the random number generator 3) comprises a decryption key and said using comprises decrypting data (i.e., decrypting device uses the extracted temporary key and decrypts the body portion 8)(Col. 8, lines 7-20).

Regarding claim 12, Shimizu discloses a display circuit for use in a display unit (i.e., portable PC), said display circuit comprising:

a non-volatile memory (i.e., storage device 12) storing an encrypted key, wherein said encrypted key is generated from an unencrypted key according to an encryption protocol (Col.); and

Shimizu does not expressly disclose and integrated circuit coupled to a non-volatile memory.

However, Ashe discloses an integrated circuit (i.e., DSP) coupled to said non-volatile memory (i.e., EPROM), said integrated circuit receiving said key in encrypted form (i.e., Zi, encrypted Kc) and decrypting said key to generate a decrypted key (i.e., Kc, decrypted Zi), said integrated circuit using said decrypted key (i.e., reading the encrypted program Y with the customer decryption algorithm module 23)(Col. 2, lines 65-67 and Col. 3, lines 1-10).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Shimizu with the teachings of Ashe to include an integrated processing unit such as a Digital Signal Processor (DSP), that has both the proprietor's unique algorithm (i.e., unencrypted key), master algorithm (i.e., encryption protocol), and master key (i.e., the key to encrypt the unencrypted key) with the motivation to protect information stored in a memory device (Ashe, Col. 1, lines 1-10).

Regarding claim 13, Shimizu discloses wherein said integrated circuit comprises a key encryption circuit (i.e., encrypting device 10) receiving said unencrypted key (i.e., temporary key), said key encryption circuit generating said encrypted key from said unencrypted key according to said encryption protocol (i.e., the encrypting device 10 encrypts the temporary key using the master key)(Col. 16, lines 8-55).

Regarding claim 14, Shimizu does not expressly disclose wherein said integrated circuit further comprises: a memory receiving said encrypted key; and a port coupled to said memory, said port receiving said encrypted key from said memory and sending said encrypted key to a master block, wherein said master block stores said encrypted key in said non-volatile memory.

However, Ashe discloses wherein said integrated circuit further comprises: a memory receiving said encrypted key (i.e., memory 11); and a port coupled to said memory, said port receiving said encrypted key (i.e., Zi, the encrypted Kc) from said

memory and sending said encrypted key to a master block (i.e., DSP), wherein said master block stores said encrypted key in said non-volatile memory (i.e., EPROM 11)(Col. 2, lines 49-67 and Col. 3, lines 1-15).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Shimizu with the teachings of Ashe to include a non-volatile memory such as EPROM that both receives and stores the encrypted key until it is needed with the motivation to protect information stored in a memory device (Ashe, Col. 1, lines 1-10).

Regarding claim 15, Shimizu discloses wherein said integrated circuit further comprises a key decryption circuit (i.e., decrypting device 20) receiving said encrypted key (i.e., header portion 11), and generating said decrypted key (i.e., original temporary key) according to said encryption protocol (i.e., master key)(Col. 8, lines 7-20).

Claims 5-6, 7, 9, and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shimizu et al., (U.S. Patent No. 6,085,323 and Shimizu hereinafter), in view of Ashe, (U.S. Patent No. 6,014,745 and Ashe hereinafter), in further view of Kuno et al., (U.S. Patent No. 6,584,552 and Kuno hereinafter).

Regarding claim 5, Shimizu discloses a method of using an unencrypted key in a display unit (Col. 7, lines 3-55).

Shimizu does not expressly disclose receiving said unencrypted key in said display unit.

However, Kuno discloses receiving said unencrypted key in said display unit (Col. 19, lines 3-67 and Col. 20, lines 1-67);

Shimizu further discloses said method comprising:

encrypting said key according to an encryption protocol to generate an encrypted key (i.e., the encrypting device 10 encrypts the transferred temporary key using a master key stored in a master key memory 9)(Col. 7, lines 13-22);

storing said encrypted key in a non-volatile memory contained within said display unit (i.e., the header portion 11 and the body portion 8 is stored in the storage device 12)(Col. 7, lines 26-30);

retrieving said key into an integrated circuit when said key is required for use, wherein said integrated circuit is contained within said display unit, decrypting said key in said integrated circuit, and using said key (Col. 8, lines 7-19).

Shimizu does not expressly disclose decrypting and using the unencrypted key in the same integrated circuit.

However, Ashe discloses:

retrieving said encrypted key (i.e., Zi, the encrypted Kc) into an integrated circuit (i.e., DSP, Digital Signal Processor) when said unencrypted key is required for use, decrypting said encrypted key in said integrated circuit to generate said unencrypted key (i.e., deciphering Zi with the master decryption algorithm module21), and using said unencrypted key (i.e., after the key Kc is deciphered, the DSP reads the encrypted

program y with the customer decryption algorithm module 23)(Col. 2, lines 65-67 and Col. 3, lines 1-10).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Shimizu with the teachings of Ashe to include an integrated processing unit such as a Digital Signal Processor (DSP), that has both the proprietor's unique algorithm (i.e., unencrypted key), master algorithm (i.e., encryption protocol), and master key (i.e., the key to encrypt the unencrypted key) with the motivation to protect information stored in a memory device (Ashe, Col. 1, lines 1-10) and to modify the teachings of Shimizu and Ashe with the teachings of Kuno to include receiving an unencrypted key in the display unit with the motivation to securely use the protected/encrypted data and determining the access rights (Kuno, Col. 19, lines 7-67).

Regarding claim 6, both Shimizu and Ashe disclose some sort of display unit in portable PC and IBM PC.

Shimizu or Ashe does not expressly disclose discloses wherein said display unit comprises an analog display unit.

However, Kuno discloses wherein said display unit comprises an analog display unit (i.e., analog outputting means for outputting data in analog manner)(Col. 11, lines 24-27).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Shimizu and Ashe with the

teachings of Kuno to include an analog outputting means for outputting data in analog manner with the motivation to provide the capability to display data in analog/digital manner interchangeably (Kuno, Col. 11, lines 24-60).

Regarding claim 7, Shimizu discloses wherein said display unit comprises a digital display unit (i.e., DVD, Digital Video Disk)(Col. 22, lines 50-67).

Regarding claim 9, Shimizu does not expressly disclose further comprising authenticating a source of data.

However, Ashe discloses further comprising authenticating a source of data (i.e., the contractor providing cash such as a bank), wherein said authenticating is performed using said unencrypted key based on data sent and received on a path connected to said display unit (i.e., the user enters PIN via the keypad and it is verified that the entered PIN is the same as the decrypted key and allow the card holder to conduct transactions and obtain cash via dispenser)(Col. 3, lines 15-38 and Col. 4, lines 1-15).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Shimizu with the teachings of Ashe to include a microprocessor similar to DSP as part of a smart card system, the memory, equipped with conductors, mounted on a card to be inserted in a slot with the motivation to allow a machine such as a cash machine having a microprocessor mounted within it to read the memory and verify that the key card holder enters is the

same as the encrypted key and allow the card holder to conduct transaction (Ashe, Col. 3, lines 15-36).

Regarding claim 11, Shimizu discloses wherein a master block external to said display unit sends said unencrypted key (i.e., the temporary key generated by the random number generator is transferred to and encrypted in the encrypting device 10 of IC card 5), said method further comprising sending said encrypted key to said master block, wherein said mater block stores said encrypted key in said non-volatile memory (i.e., storage device 12)(Col. 7, lines 10-27).

Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Shimizu et al., (U.S. Patent No. 6,085,323 and Shimizu hereinafter) and Ashe, (U.S. Patent No. 6,014,745 and Ashe hereinafter), in view of Klein et al., (U.S. Patent No. 6,134,655 and Klein hereinafter), in further view of Philips Semiconductors: The I2C-Buss Specification, Version 2.1, Document Order No. 9398 393 40011.

The teachings of Shimizu and Ashe have been discussed before.

Regarding claim 10, Shimizu or Ashe does not expressly disclose wherein said path is implemented using I2C protocol.

However, Klein discloses wherein said path is implemented using I2C protocol (Col. 29, lines 8-67).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Shimizu and Ashe with the teachings of Klein to include I2C protocol to send and receive various security commands with the motivation to provide for a simple fault diagnosis and debugging to trace malfunctions immediately (Philips Semiconductors: The I2C Bus Specification, Page 4).

Claims 8 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shimizu et al., (U.S. Patent No. 6,085,323 and Shimizu hereinafter) and Ashe, (U.S. Patent No. 6,014,745 and Ashe hereinafter), in view of Muratani et al., (U.S. Patent No. 6,061,451 and Muratani hereinafter).

The teachings of Shimizu and Ashe have been discussed before.

Regarding claim 8, Shimizu or Ashe does not expressly disclose receiving a display signal in encrypted format.

However, Muratani discloses further comprising receiving a display signal containing a plurality of pixel data elements in an encrypted format (i.e., scrambled data), wherein decryption of said plurality of pixel data elements requires said unencrypted key, wherein said unencrypted key is used to decrypt said plurality of pixel data elements (Col. 13, lines 49-67 and Col. 14, lines 1-55).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Shimizu and Ashe with the

teachings of Muratani to include receiving data in encrypted format with the motivation to protect decrypted data transmitted or outputted with being encrypted (Muratani, Col. 1, lines 7-16).

Regarding claim 16, Shimizu or Ashe does not expressly disclose receiving a display signal in encrypted format.

However, Muratani discloses further comprising:

a receiver receiving a plurality of digital data elements encoded in a display signal, wherein said digital data elements represent a plurality of pixel data elements in an encrypted form (i.e., scrambled data), said plurality of pixel data elements representing an image (i.e., video signal), and a data decryption circuit (i.e., descrambled circuit 114) receiving said plurality of digital data elements and generating said plurality of pixel data elements, wherein said image is generated on a display screen (i.e., monitor 104) based on said plurality of pixel data elements (Col. 13, lines 49-67 and Col. 14, lines 1-55).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Shimizu and Ashe with the teachings of Muratani to include receiving plurality of pixel data elements representing an image in encrypted format with the motivation to protect decrypted data transmitted or outputted with being encrypted (Muratani, Col. 1, lines 7-16).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Gammie et al., (U.S. Patent No. 5,237,610).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (703) 305-8749. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

A. Sherkat

Arezoo Sherkat
Patent Examiner
Technology Center 2100
Feb 27, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100